Office of the
Privacy Commissioner
of Canada

Anti-spam law's changes to Canadian federal privacy law:

A guide for businesses doing e-marketing

Table of Contents

Today's economy and society are growing increasingly digital and connected. An organization can promote itself to thousands of contacts with a simple click.

While it is technically possible to collect thousands and thousands of addresses for marketing purposes or to buy a list from a third party, doing so blindly comes at a risk, both under the law and to an organization's brand.

On July 1, 2014, Canada's anti-spam law (CASL), Canada's law against spam and other electronic threats, came into force. This included amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the federal private sector privacy law which covers the collection, use and disclosure of personal information in the course of commercial activities.

The scope of this guide

This guide is aimed at informing organizations about the Office of the Privacy Commissioner of Canada's (OPC) mandate around electronic address harvesting.

It seeks to answer questions organizations may have about how to ensure they comply with PIPEDA when it comes to address harvesting.

Who is responsible for what under CASL?

Our Office shares responsibility for enforcing CASL with the Canadian Radio-television and Telecommunications Commission (CRTC) and the federal Competition Bureau.

The CRTC is responsible for investigating the sending of unsolicited commercial electronic messages, the alteration of transmission data and the installation of software without consent.

The Competition Bureau addresses false or misleading representations and deceptive marketing practices in the electronic marketplace.

For details about the full range of matters dealt with under CASL, including those by organizations other than the OPC, please visit **www.fightspam.gc.ca**

Address harvesting

What are PIPEDA's address harvesting provisions about?

Address harvesting is referred to in PIPEDA as collecting electronic addresses, such as email addresses, through the use of a computer program that may involve scraping websites or generating a list of email addresses.

The restrictions related to address harvesting are highly relevant to organizations of all shapes and sizes in all sectors. An organization has a responsibility to ensure that all individuals receiving its electronic messages have provided appropriate consent for the collection and use of their address for marketing and other purposes.

We don't engage in address harvesting, so what do these changes mean for my business?

PIPEDA requires that organizations be accountable for how they collect, use and disclose personal information, including electronic addresses, in the course of their commercial activities. This includes ensuring that they have obtained informed consent to collect and use individuals' electronic addresses, even if they obtained the addresses from a third party supplier.

If an organization engages in address harvesting or obtains and uses a list that has been compiled through address harvesting, it runs a real risk that it will be collecting electronic addresses without consent, in contravention of PIPEDA. Although there are certain exceptions under PIPEDA where personal information can be collected without consent, these exceptions by and large do not apply to address harvesting.

Section 7.1(2) of PIPEDA states that certain exceptions for the collection and use of personal information without consent **do not apply with respect to:**

- (a) the collection of an individual's electronic address, if the address is collected by the use of a computer program that is designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses; or
- (b) the use of an individual's electronic address, if the address is collected by the use of a computer program described in paragraph (*a*).

What if I hired a supplier to do something like email marketing? Is my organization accountable for work done by a third party on my behalf?

In a word, yes. Even in cases where your organization didn't collect or generate e-mail address lists for marketing purposes, your organization is responsible under PIPEDA for ensuring that appropriate consent was obtained.

If your organization acquired and used a list from a vendor who gathered the addresses without consent, or if you hired a company to run a campaign and it used addresses collected without consent, then your organization could be found in contravention of PIPEDA.

What are the key steps I need to take to avoid contravening PIPEDA when collecting addresses?

Basically, individuals must consent to having their e-mail addresses collected and used for marketing purposes.

This means individuals need to be clearly and accurately informed at the point of collection about how their addresses will be used, and they must be able to opt out of receiving messages at any time in the future. More details about consent are included later in this document.

If people post their addresses online, does that mean I can collect them for commercial purposes?

No. It cannot be assumed that those people whose addresses are posted are interested in commercial offers.

Addresses may be posted online for many different purposes. For example:

- An individual may solicit feedback from people interested in the subject of a blog or article they have written;
- A club or community group may wish to facilitate contact amongst its members to organize events;
- A charitable organization may do so to receive donations; and
- Organizations may include employee email addresses on a contact page or staff directory to enable communication with employees regarding matters related to their employment or profession.

Spamming: cheap, yet costly

While sending out unsolicited messages to thousands may be a cheap way of getting a name out, organizations need to consider if spam is a desirable calling card.

Consider for example that in a 2012 public opinion survey conducted for our Office, 73% of Canadians who used the Internet were concerned about companies using their information to send them spam.

Businesses and organizations that comply with PIPEDA and CASL—and follow due diligence to ensure that third parties they work with do the same—will benefit by not being seen as spammers.

To be safe, assume nothing and ensure that an address collected for commercial purposes is done so with the individual's full consent.

As an organization working with third parties engaging in electronic marketing, what are the key steps we need to take to avoid contravening PIPEDA?

If you're sending messages yourself using a list directly from a vendor, ask the company how the addresses, and how consent for their use, was obtained. It is ***your*** responsibility to confirm if the company you are working with is aware of PIPEDA and abiding by its provisions. In other words, while another company may be doing the work, it is doing it on your behalf, and you remain accountable.

If you're working with a marketing firm, ask them to explain—in detail—where they get the e-mail addresses they will use to promote your business.

If the firm's list was purchased from a third party, ask the marketers to explain how the e-mail addresses were originally gathered and how consent was obtained.

You should also ask the vendor or marketing firm to explain how the lists are kept up to date and how organizations purchasing and using its lists are kept informed of changes.

For example, how do they ensure that new addresses are only added to a list when appropriate consent has been obtained and that addresses are promptly deleted from a list when consent has been withdrawn by an individual "unsubscribing" from the receipt of future emails?

In all cases, make it clear and keep a written record, indicating that you don't want to have your messages sent to people who have not consented to providing their email addresses or receiving marketing messages.

After all, given people's general distaste for receiving spam, what organization would want to run the risk of being seen as a spammer?

Collecting email addresses and selling lists to organizations and marketers is part of my business. What should I know about consent?

In this situation, a list vendor may be collecting addresses, but not sending messages to them. While the CRTC is responsible for CASL's rules regarding the sending of commercial electronic messages and appropriate consent, PIPEDA applies to the collection, use and disclosure of personal information, which includes individuals' email addresses.

Generally, under PIPEDA, an organization is required to inform individuals in a meaningful way of the purposes for the collection, use or disclosure of personal information (and yes, an email address, even a business email address, is considered personal information under PIPEDA).

Further, individuals' consent should be obtained before or at the time of collection, and then renewed when a new use of their personal information is identified.

In addition, organizations should enable individuals to withdraw consent to the use of their personal information at any time, subject to legal or contractual restrictions and reasonable notice.

And so, if a list vendor is collecting email addresses in bulk through electronic means and then selling them without informing individuals and obtaining appropriate consent, it could find itself contravening several of PIPEDA's provisions.

Hypothetical scenarios showing potential pitfalls

The following hypothetical scenarios highlight how well-meaning individuals and organizations could put themselves at risk of being investigated for address harvesting and/or collection and using electronic addresses without consent under PIPEDA:

Getting the word out to thousands in a click … but where did the addresses come from?

A small business selling customized smartphone cases was seeking an affordable way to get word of its product out to thousands of individuals. It purchased a list of email addresses from a vendor. The vendor, however, generated the list by using "web crawler" software to mine the Internet for posted email addresses and therefore did not have individuals' consent.

Collecting addresses for one purpose, then selling them for another

Several consumers submit spam reports claiming that a car parts and services company is sending emails to them when they did not provide the company with their email addresses. All are members of the same car aficionados' website and provided their email addresses for the members' password protected section of the site. It appears that the website may have sold an electronic list of its members' addresses to the car parts and services company without the members' consent to do so.

Downloading open data

A list vendor becomes aware that an organization employing thousands of people and committed to the principle of "open data" allows people to download thousands of employee email addresses with little more than a click. The vendor erroneously assumes that the addresses, as they are associated with an employer, are not subject to PIPEDA. However, business contact information may be subject to the Act if it is being collected, used or disclosed for a purpose other than communicating or facilitating communication with an individual in relation to their employment, business or profession.

Not collecting, but generating addresses

A tech-savvy entrepreneur wants to sell marketers lists of email addresses, but wants to avoid what he sees as 'stealing' them from individuals whose contact information is posted on the web. So, he uses a tool that generates addresses using common names (as found in a phone book) and matching them with common email service provider domains. His overhead is low, so many are enticed by the list he offers at very low prices—especially given his claim that the addresses weren't 'scraped' from the web. Still, he did not get individuals' consent for use of their email addresses.

Collecting addresses and then selling them for commercial use – without consent

A website offers visitors the chance to win an all-expenses paid trip to an exotic location. To get a chance to win, people are asked to provide their email addresses and the lucky winner will receive the good news in their in box. A week later, the winner indeed gets an email informing her that she has won and the prize is legitimate. Shortly afterward though, she and others who provided their addresses begin receiving messages offering products and services from unknown senders. This is because the addresses gained were collected and then sold, without user consent, for use by companies for commercial purposes.

Online resources
Please visit our website at www.priv.gc.ca.
Follow us on Twitter: @privacyprivee

Contact us
Our Information Centre is open weekdays from 8:30 a.m. to 4:30 p.m. ET.
Toll-free: 1-800-282-1376
Phone: (819) 994-5444
Fax: (819) 994-5424
TTY: (819) 994-6591

Mailing address
Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H